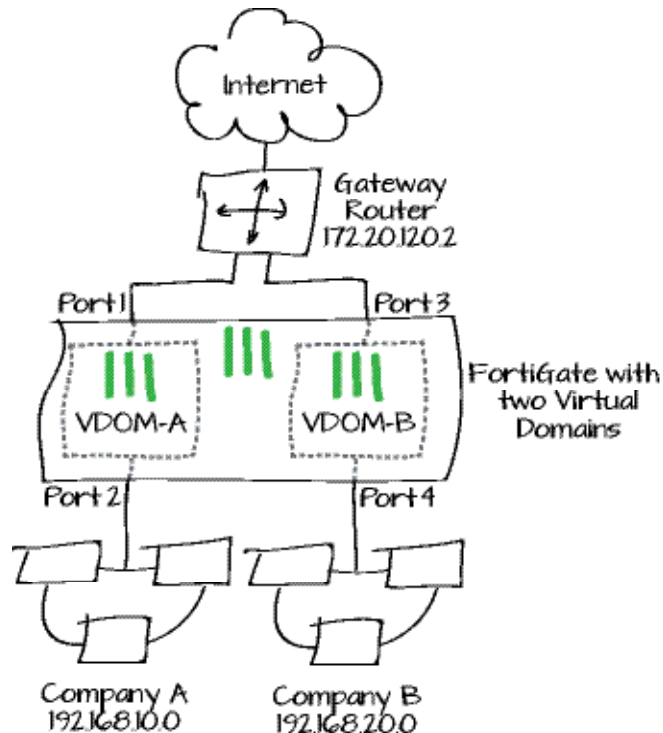


Using VDOMs to host two FortiOS instances on a single FortiGate unit

Virtual Domains (VDOMs) can be used to divide a single FortiGate unit into two or more virtual instances of FortiOS that function as independent FortiGate units. This example simulates an ISP that provides Company A and Company B with distinct Internet services. Each company has its own VDOM, IP address, and internal network.

1. Switching to VDOM mode and creating two VDOMS
2. Assigning interfaces to each VDOM
3. Creating administrators for each VDOM
4. Creating a basic configuration for VDOM-A
5. Creating a basic configuration for VDOM-B
6. Connecting the gateway router
7. Results



1. Switching to VDOM mode and creating two VDOMS

Go to **System > Dashboard > Status.**

In the **System Information** widget, find **Virtual Domain** and select **Enable.**



You will be required to re-login after enabling **Virtual Domain** due to the GUI menu options changing.

System Information	
HA Status	Standalone [Configure]
Host Name	FGT60C3G10016011 [Change]
Serial Number	FGT60C3G10016011
System Time	Fri Oct 24 08:45:13 2014 (FortiGuard) [Change]
Firmware Version	v5.2.1,build618 (GA) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /1 in Total [Details]
Uptime	0 day(s) 0 hour(s) 33 min(s)
Virtual Domain	Enabled [Disable]

Go to **Global > VDOM > VDOM.**

Create two VDOMS: *VDOM-A* and *VDOM-B*. Leave both VDOMs as **Enabled**, with **Operation Mode** set to **NAT**.

Name	<input type="text" value="VDOM-A"/>
Enable	<input checked="" type="checkbox"/>
Operation Mode	<div> NAT</div>
Comments	<div><input type="text" value="Write a comment..."/></div> <div>0/255</div>

Name	<input type="text" value="VDOM-B"/>
Enable	<input checked="" type="checkbox"/>
Operation Mode	<div> NAT</div>
Comments	<div><input type="text" value="Write a comment..."/></div> <div>0/255</div>

2. Assigning interfaces to each VDOM

Go to **Global > Network > Interfaces**.

Edit **port1** and add it to VDOM-A.
Set **Addressing Mode** to **Manual**
and assign an **IP/Network Mask**
to the interface (in the example,
172.20.120.10/255.255.255.0).

Name	port1(00:09:0F:B0:EB:F0)
Alias	<input type="text"/>
Link Status	Down
Type	Physical Interface
Virtual Domain	VDOM-A
Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> One-Arm Sniffer <input type="radio"/> Dedicate to FortiA
IP/Network Mask	<input type="text" value="172.20.120.10/255.255.255.0"/>
IPv6 Address	<input "::="" 0"="" type="text" value=""/>

Edit **port2** and add it to VDOM-A.
Set **Addressing Mode** to **Manual**,
assign an **IP/Network Mask**
to the interface (in the example,
192.168.10.1/255.255.255.0), and set
Administrative Access to **HTTPS**,
PING, and **SSH**. Enable **DHCP**
Server.

Name	port2(00:09:0F:B0:EB:F1)				
Alias	<input type="text"/>				
Link Status	Down				
Type	Physical Interface				
Virtual Domain	VDOM-A				
Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> Dedicate to FortiAP/FortiSwitch				
IP/Network Mask	<input type="text" value="192.168.10.1/255.255.255.0"/>				
IPv6 Address	<input "::="" 0"="" type="text" value=""/>				
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP				
	<input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET <input type="checkbox"/> FCT-Access				
IPv6 Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP				
	<input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET				
DHCP Server	<input checked="" type="checkbox"/> Enable				
Address Range	<div><div>Create New </div><table><thead><tr><th>Starting IP</th><th>End IP</th></tr></thead><tbody><tr><td>192.168.10.2</td><td>192.168.10.254</td></tr></tbody></table></div>	Starting IP	End IP	192.168.10.2	192.168.10.254
Starting IP	End IP				
192.168.10.2	192.168.10.254				
Netmask	<input type="text" value="255.255.255.0"/>				

Edit **port3** and add it to VDOM-B.
Set **Addressing Mode** to **Manual**
and assign an **IP/Network Mask**
to the interface (in the example,
172.20.120.20/255.255.255.0).

Name	port3(00:09:0F:B0:EB:F2)
Alias	<input type="text"/>
Link Status	Down
Type	Physical Interface
Virtual Domain	VDOM-B
Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> One-Arm Sniffer <input type="radio"/> Dedicate to FortiAP/f
IP/Network Mask	<input type="text" value="172.20.120.20/255.255.255.0"/>
IPv6 Address	<input "::="" 0"="" type="text" value=""/>

Edit **port4** and add it to VDOM-B.
Set **Addressing Mode** to **Manual**,
assign an **IP/Network Mask**
to the interface (in the example,
192.168.20.1/255.255.255.0), and set
Administrative Access to **HTTPS**,
PING, and **SSH**. Enable *DHCP*
Server.

Interface Name	internal4(00:09:0F:DF:43:4D)						
Alias	<input type="text"/>						
Link Status	Down						
Type	Physical Interface						
Virtual Domain	VDOM-B						
Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> One-Arm Sniffer <input type="radio"/> Dedicated to Extension Device						
IP/Network Mask	<input type="text" value="192.168.20.1/255.255.255.0"/>						
IPv6 Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP						
IPv6 Address/Prefix	<input "::="" 0"="" type="text" value=""/>						
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> FCT-Access <input type="checkbox"/> Auto IPsec Request						
IPv6 Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP <input type="checkbox"/> SSH <input type="checkbox"/> SNMP						
DHCP Server	<input checked="" type="checkbox"/> Enable						
Address Range	<div><div>Create New Edit Delete</div><table><thead><tr><th>Starting IP</th><th>End IP</th></tr></thead><tbody><tr><td>192.168.20.2</td><td>192.168.20.254</td></tr></tbody></table></div>			Starting IP	End IP	192.168.20.2	192.168.20.254
Starting IP	End IP						
192.168.20.2	192.168.20.254						
Netmask	<input type="text" value="255.255.255.0"/>						

3. Creating administrators for each VDOM

Go to **Global > Admin > Administrators**.

Create an administrators for VDOM-A, called *a-admin*. Set **Type** to **Regular**, set a password, and set **Admin Profile** to **prof_admin**.

Administrator	<input type="text" value="a-admin"/>		
Type	<input checked="" type="radio"/> Regular <input type="radio"/> Remote <input type="radio"/> PKI		
Password	<input type="password" value="....."/>		
Confirm Password	<input type="password" value="....."/>		
Comments	<input type="text" value="Write a comment..."/> 0/255		
Admin Profile	<input type="text" value="prof_admin"/>		
Virtual Domain	<input type="text" value="VDOM-A"/>		

Create an administrators for VDOM-B, called *b-admin*. Set **Type** to **Regular**, set a password, and set **Admin Profile** to **prof_admin**.

Administrator	<input type="text" value="b-admin"/>		
Type	<input checked="" type="radio"/> Regular <input type="radio"/> Remote <input type="radio"/> PKI		
Password	<input type="password" value="....."/>		
Confirm Password	<input type="password" value="....."/>		
Comments	<input type="text" value="Write a comment..."/> 0/255		
Admin Profile	<input type="text" value="prof_admin"/>		
Virtual Domain	<input type="text" value="VDOM-B"/>		



Make sure to remove the **root** VDOM from both administrator accounts.

4. Creating a basic configuration for VDOM-A

Go to **Virtual Domains** and select **VDOM-A**.

Go to **System > Network > Routing**.

Create a default route for the VDOM. Set **Destination IP/Mask** to *0.0.0.0/0.0.0.0*, set **Device** to **port1**, and set **Gateway** to the IP of the gateway router (in the example, *172.20.120.2*).

Destination IP/Mask	<input type="text" value="0.0.0.0/0.0.0.0"/>
Device	<input type="text" value="internal1 (port1)"/>
Gateway	<input type="text" value="172.20.120.2"/>

Connect a PC to port2. Using HTTPS protocol, browse to the IP set for port2 and log into VDOM-A using the a-admin account (in the example, *192.168.10.1*).

Go to **Policy & Objects > Policy > IPv4**

Create a policy to allow Internet access. Set **Incoming Interface** to **port2** and **Outgoing Interface** to **port1**. Ensure **NAT** is turned **On**.

Incoming Interface	<input type="text" value="internal2 (port2)"/>	+
Source Address	<input type="text" value="all"/>	+
Source User(s)	<input type="text" value="Click to add..."/>	
Source Device Type	<input type="text" value="Click to add..."/>	
Outgoing Interface	<input type="text" value="internal1 (port1)"/>	+
Destination Address	<input type="text" value="all"/>	+
Schedule	<input type="text" value="always"/>	
Service	<input type="text" value="ALL"/>	+
Action	<input type="text" value="ACCEPT"/>	
Firewall / Network Options		
<input checked="" type="checkbox"/> NAT		
<input checked="" type="radio"/> Use Outgoing Interface Address	<input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool	<input type="text" value="Click to add..."/>	

5. Creating a basic configuration for VDOM-B

If you have logged out o the FortiGate unit, log back in.

Go to **Virtual Domains** and select **VDOM-B**.

Go to **System > Network > Routing**

Create a default route for the VDOM. Set **Destination IP/Mask** to 0.0.0.0/0.0.0.0, set **Device** to **port3**, and set **Gateway** to the IP of the gateway router (in the example, 172.20.120.2).

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	internal3 (port3) ▼
Gateway	172.20.120.2

Connect a PC to port4. Using HTTPS protocol, browse to the IP set for port4 and log into VDOM-B using the a-admin account (in the example, https://192.168.10.1).

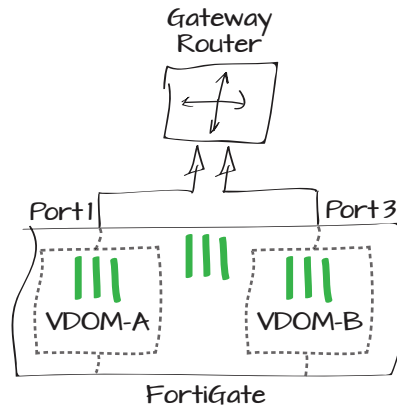
Go to **Policy & Objects > Policy > IPv4**

Create a policy to allow Internet access. Set **Incoming Interface** to **port2** and **Outgoing Interface** to **port1**. Ensure **NAT** is turned **On**.

Incoming Interface	internal4 (port4) ▼	⊕
Source Address	all ▼	⊕
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	internal3 (port3) ▼	⊕
Destination Address	all ▼	⊕
Schedule	always ▼	
Service	ALL ▼	⊕
Action	ACCEPT ▼	
Firewall / Network Options		
<input checked="" type="checkbox"/> NAT		
<input checked="" type="radio"/> Use Outgoing Interface Address	<input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool	Click to add...	

6. Connecting the gateway router

Connect port 1 and port3 of the FortiGate unit to the gateway router to allow Internet traffic to flow.

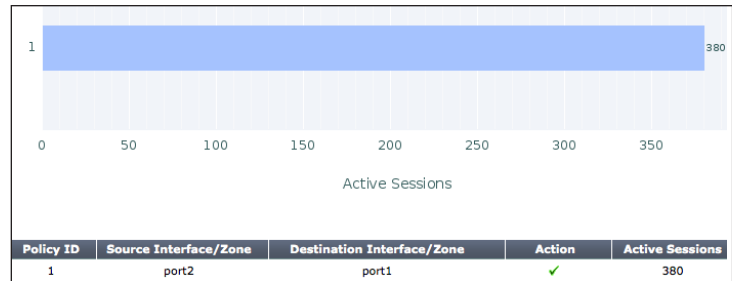


7. Results

Connect to the Internet from the company A and company B networks and then log into the FortiGate unit

Go to **Virtual Domains** and select **VDOM-A**.

Go to **Policy & Objects > Monitor > Policy Monitor** to view the sessions being processed on VDOM-A.



Go to **Policy & Objects > Monitor > Policy Monitor** to view the sessions being processed on VDOM-B.

